Secure bits with quantum pseudo-telepathy

Secure Bits with Quantum Pseudo-Telepathy

Master Thesis
Tobias Ambühl

Department of Computer Science
Swiss Federal Institute of Technology (ETH) Zurich

January 20, 2009

Faculty	:	Group of Quantum Information Prof. Dr. Stefan Wolf
Author	:	Tobias Ambühl tambuehl@student.ethz.ch
Advisor	:	Prof. Dr. Stefan Wolf wolfst@inf.ethz.ch
Mentor	:	Dejan Daniel Dukaric ddukaric@ethz.ch
	&	Esther Hänggi esther.haenggi@inf.ethz.ch

Abstract

Motivated by the concept of quantum pseudo-telepathy games as well as by quantum key distribution protocols such as [1], the security of which is based on the non-signaling principle, we try to answer the question wheather it is possible to generate a perfectly secure, shared bit between two parties by a single usage of quantum correlations and a performance of local operations on the input and output.

We provide both parties with some prior shared entanglement and the possibility of postselection, e.g. discard of inputs and outputs, aiming to prevent any eavesdropper bound by the non-signaling condition from successfully performing an attack.

After, in a first step, defining the framework and setting up the requirements we are going to see that quantum mechanics does not allow for a physical simulation of such correlations.

For the case of binary output we will even see that, in order to make perfectly correlated bits perfectly secure, we would need maximal non-local correlations which also prohibits a quantum physical representation.

Contents

1 Introduction

It is well known how to generate common secret shared bits for key agreement using quantum mechanics, as for example in [1]. Those schemes have in common that, in order to achieve a certain degree of secrecy, a part of the input gets discarded.
However, among the results of the magic square game (see Definition 3.1 for more details) resides a shared bit, the intersection bit, which seems to be secret up to the moment of announcement by Alice and Bob. It turns out to be a natural question to ask wheather Alice and Bob, by not publishing any information, would share a perfectly secret bit which could further be used for key agreement. This would mean that the usage of a quantum-physical system in combination with some local operations as for example retention or discard of input or output information would equip us with a single usage device for generating common secret bits. So in the rest of the paper we are going to investigate the demands on those devices and we are going to see that, unfortunately, quantum mechanics excludes a physical representation of those.
We will use the terms of boxes with input and outputs, meaning that we have some prior shared entanglement on which measurement in a certain base (input) can be performed, giving rise to measurement results (output).

2 Preliminaries

In the context of bipartite quantum systems, two players named Alice and Bob share joint quantum state ρ on $\mathcal{H}$, where

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$$

with $\mathcal{H}_A$ being Alice's Hilbert space and $\mathcal{H}_B$ being Bob's, respectively. Although we have a finite number of dimensions we do not restrict ourselves on its number, so we can assume that ρ is in a pure state and that its density operator ρ, defined [7] by

$$\rho = |\psi\rangle \ \langle\psi|,$$

has the property that $tr(\rho^2) = 1$. We further assume that Alice and Bob perform projective measurements, described by two sets of projection operators, namely $\{E_\alpha\}$ where $E_\alpha = \tilde{E_\alpha} \otimes I$, acting on Alice's system and $\{E_\beta\}$ where $E_\beta = \tilde{E_\beta} \otimes I$ acting on Bob's system, for which holds that

$$\begin{aligned} \sum_\alpha E_\alpha &= 1 \\ \sum_\beta E_\beta &= 1 \end{aligned}$$

as well as

$$E_\alpha E_{\alpha'} = \begin{cases} E_\alpha & if\ \alpha = \alpha' \\ 0 & otherwise \end{cases} \tag{1}$$

When applied on state ρ, the possible outcome of a measurement can be described as follows:

$$Pr(\alpha\beta) = tr(E_\alpha E_\beta \rho). \tag{2}$$

In the case ρ being a pure state, this probability can be written equivalently as

$$Pr(\alpha\beta) = \langle\psi|E_\alpha E_\beta|\psi\rangle. \tag{3}$$

3 Quantum Pseudo-Telepathy Games

To explain the concept of quantum pseudo-telepathy games, consider the following, illustrative, scenario, where Alice and Bob claim to have telepathic powers [2]. In order to prove this, Alice and Bob build up a large distance between them and ask Xavier and Yolanda to name values to them, i.e. Xavier to Alice a value $x \in X$ and Yolanda to Bob a value $y \in Y$ having the same distribution. Upon having received their inputs simultaneously, Alice and Bob immediately output "yes" if they both got the same input value or "no" otherwise. Because of the large distance, the possibility of communication, in particular of agreeing on a specific output, is impossible. This means that in case Alice and Bob winning this game with overwhelming probability, the only explanation in a classical world would be telepathy.
The game described above cannot be won with the help of quantum mechanics, but there are other similar games for which there exists no classical winning strategy, whereas the game can be won if some prior entanglement is shared. The term *pseudo telepathy* is rooted in the fact that for any classical observer there is no other explanation than telepathy, while in the world of quantum mechanics it all can be described physically.

Definition 3.1. *[2] A two partite game is defined as a sextuple $G = \langle X, Y, A, B, P, W\rangle$, where*

- *X and Y are the input sets for Alice and Bob.*
- *A and B are the output sets.*
- *$P \subseteq X \times Y$ is a predicate on $X \times Y$, called* promise *or probability distribution on $X \times Y$. If not stated differently, X and Y are uniformly distributed.*
- *$W \subseteq X \times Y \times A \times B$ is also a predicate, called the* winning condition*.*

Definition 3.2. *A strategy between Alice and Bob is called a* classical strategy *if their output only depends on the deterministic mappings $X \to A$ and $Y \to B$ and some shared randomness. It is called a* quantum strategy *if Alice and Bob share some prior entanglement on which they can perform measurements in order to get their output values.*

Definition 3.3. *[2] We call a game as defined in 3.1 a pseudo-telepathy game if there is no winning strategy with success probability equal to 1 for Alice and Bob as classical players, yet it admits such a winning strategy for Alice and Bob following a quantum strategy.*

Note that for a quantum pseudo telepathy game we require a quantum winning strategy with success probability equal to 1. As an example please have a look at the Magic Square Game described in subsection 3.1.

3.1 Magic Square Game

A magic square, in the context of quantum pseudo telepathy games, is a binary matrix M of dimension 3×3 where the parity of all rows is even and the parity of all columns is odd. In order to see that such a matrix is magic indeed, lets consider the following matrix:

$$M = \begin{matrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & x \end{matrix} \tag{4}$$

If $x = 0$ the parity condition of the third column, if $x = 1$ the parity condition of the third row is violated.
The magic square game can formally be described as $G = \langle X, Y, A, B, W \rangle$ with

- $X = Y = \{1, 2, 3\}$
- $A = B = \{0, 1\}^3$ (Basically, Alice is asked to output the x-th row and Bob is asked to output the y-th column). Let, for example, $a(i) \in \{0, 1\}$ be the i-th bit of Alice's output row.
- W is is fulfilled, if
  - Alice's row has even parity: $a(3) = a(1) \oplus a(2)$
  - Bob's column has odd parity: $b(3) = 1 \oplus b(1) \oplus b(2)$
  - row and column agree on intersection bit: $a(y) = b(x)$

As we have seen, such a magic square cannot exist. This means that the best strategy for classical players is to assign binary values to eight of the nine entries of the magic square, as for example in (4), admitting a success probability of 8/9. But anyhow, there is a quantum winning strategy as described in [2]. First, Alice and Bob share the entangled state

$$|\psi\rangle = \frac{1}{2}|0011\rangle - \frac{1}{2}|0110\rangle - \frac{1}{2}|1001\rangle + \frac{1}{2}|1100\rangle, \tag{5}$$

where the first two qubits belong to Alice and the second two to Bob. Upon receiving their input, Alice and Bob apply each one of the following unitary transformations accordingly, i.e. Alice applies A_1 if her input is 1 and so on.

$$A_1 = \tfrac{1}{\sqrt{2}} \begin{bmatrix} i & 0 & 0 & 1 \\ 0 & -i & 1 & 0 \\ 0 & i & 1 & 0 \\ 1 & 0 & 0 & i \end{bmatrix}, B_1 = \tfrac{1}{2} \begin{bmatrix} i & -i & 1 & 1 \\ -i & -i & 1 & -1 \\ 1 & 1 & -i & i \\ -i & i & 1 & 1 \end{bmatrix}$$

$$A_2 = \tfrac{1}{2} \begin{bmatrix} i & 1 & 1 & i \\ -i & 1 & -1 & i \\ i & 1 & -1 & -i \\ -i & 1 & 1 & -i \end{bmatrix}, B_2 = \tfrac{1}{2} \begin{bmatrix} -1 & i & 1 & i \\ 1 & i & 1 & -i \\ 1 & -i & 1 & i \\ -1 & -i & 1 & -i \end{bmatrix}$$

$$A_3 = \tfrac{1}{2} \begin{bmatrix} -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix}, B_3 = \tfrac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{bmatrix}$$

After Alice and Bob have applied their transformations, they measure their bits in the computational basis, which results in the first two output bits for each. The third bit is then chosen w.r.t. parity. So if we have for example inputs $x = 2$ and $y = 3$, we get the following computation [2]:

$$(A_2 \otimes B_3)|\psi\rangle = \frac{1}{2\sqrt{2}}[|0000\rangle - |0010\rangle - |0101\rangle + |0111\rangle \\ +|1001\rangle + |1011\rangle - |1100\rangle - |1110\rangle] \tag{6}$$

The measurement result Alice and Bob obtain could be 10 and 01 which means that Alice would complement with 1 and Bob with 0, resulting in $a = 101$ and $b = 010$. As a and b agree on the intersection bit, Alice and Bob win this round of the game. The verification for all possible inputs is tedious but straightforward.

4 Framework

We want to study the following scenario, where we have three players, Alice, Bob and Eve. All three of them are non signalling, e.g., they are restricted by the impossibility of superluminal signalling. The goal of Alice and Bob is to generate a shared secret bit, about which Eve, in the role of the eavesdropper, must not be able to learn anything. We want to give Eve as much power as possible, putting her in charge of providing physical systems, on which Alice and Bob can perform measurements in order to get their shared secret bit. The behavior of those physical systems and their results of a measurement can be described as a input-output box.

Definition 4.1. *A box is a conditional probability distribution $P_{AB|XY}$ where X and Y are the input sets, A and B are the output sets of Alice and Bob. For example, $P_{A,B|X=x,Y=y}(0,1)$ denotes the probability of output $A = 0$ and $B = 1$, given $X = x$ and $Y = y$. Equivalently, we will use the notation $P(ab|xy)$ denoting the probability of $A = a$, $B = b$, given $X = x$ and $Y = y$.*

Definition 4.2. *A box is non-signalling, if the following holds:*

$$\sum_b P(ab|xy) = \sum_b P(ab|xy') = P(a|x) \ \forall a, x, y, y' \tag{7}$$

$$\sum_a P(ab|xy) = \sum_a P(ab|x'y) = P(b|y) \ \forall b, x, x', y \tag{8}$$

Concrete, a secret bit agreement protocol step might look as follows: Alice and Bob are provided a box P by Eve. They both take a $x \in X$ and a $y \in Y$ as input for the box. These input values are either form Eve, or they are chosen by Alice and Bob and then made public through an authenticated channel. After obtaining the output of the box, in order to generate a perfectly secret shared bit, Alice and Bob are allowed to perform some additional local operations, described in *Section 8*. As Eve is the one preparing and distributing the boxes, she might send boxes which do not have the input-output statistics as claimed by her. In order to prevent this, Alice and Bob can test those boxes by using a large number N of boxes, revealing and comparing (testing) the outputs for

random $N-1$ boxes and keeping the results for one box secret. In the following we will assume that the boxes have been tested and that they indeed work as expected.

5 PR Box

The Popescu Rohrlich machine is a non-local box with binary input ($X = Y = \{0,1\}$) and binary output ($A = B = \{0,1\}$) for which the following holds:

$$Pr[A \oplus B = X \cdot Y] = 1 \tag{9}$$

The next figure is an illustration of the PR box:

X \ Y		0		1	
	B / A	0	1	0	1
0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0
	1	0	$\frac{1}{2}$	0	$\frac{1}{2}$
1	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$
	1	0	$\frac{1}{2}$	$\frac{1}{2}$	0

(10)

Bell's theorem states that any box acting like the box above with a probability superior to 75% is non-local, which means that the PR box is actually maximally non-local. To see this, we can compute the expectation value of the Bell Operator:

$$E[B] = E[X_{+1}Y_{+1}] + E[X_{+1}Y_{-1}] + E[X_{-1}Y_{+1}] - E[X_{-1}Y_{-1}] \tag{11}$$

Note that $E[X_{+1}Y_{-1}]$ denotes the expected result of the multiplication of the outputs, given that Alice had input 0 (+1) and Bob had input 1 (-1). With respect to the NL box described in (10) we can now compute

$$E[B] = 1 + 1 + 1 - (-1) = 4, \tag{12}$$

which implies a maximal violation of Bell's inequality.

5.1 The eight PR Boxes

Let us now consider the set of the following non-signalling probability distributions for $r, s, t \in \{0,1\}$:

$$P_{r,s,t}(ab|xy) = \begin{cases} \frac{1}{2} & if\ r \oplus (a \oplus b) \equiv_2 (s \oplus x)(t \oplus y) \\ 0 & otherwise \end{cases} \tag{13}$$

So for $r = s = t = 0$ we have

$$P_{0,0,0}(ab|xy) = \begin{cases} \frac{1}{2} & if\ a \oplus b \equiv_2 xy \\ 0 & otherwise \end{cases} \tag{14}$$

which corresponds to the PR box described in (10).

Lemma 5.1. *Every probability distribution $P_{r,s,t}$ is equivalent to the PR box described in (10).*

Proof. For the case $P_{0,0,0}$ the lemma trivially holds. Without loss of generality, lets consider the probability distribution $P_{r,s,t}$ for some $(r,s,t) \neq (0,0,0)$. For each input-output pair (x,a) with $x \in X$ and $a \in A$ Alice just returns $(s \oplus x, r \oplus a)$ and for each input-output pair (y,b) with $y \in Y$ and $b \in B$ Bob just returns $(t \oplus y, b)$. It is easy to see that this way Alice and Bob achieve the same input-output statistics as the PR box. From now on, a PR box denotes one of the eight boxes $P_{r,s,t}$.

Lemma 5.2. *A PR can be used to generate a shared, perfectly secret bit, based on the non-signaling condition, between two players Alice and Bob.*

Assume eavesdropper Eve can learn something about the common secret bit between Alice and Bob. This means that she is able, from her perspective, to bias for example Alice's output bit $a \in A$, e.g. $Prob[a=0] = \frac{1}{2} + \varepsilon$. As Eve is in charge of distributing the boxes, she would have to prepare a box with the following behavior: $P(00|00) = \frac{1}{2} + \varepsilon$ and $P(11|00) = \frac{1}{2} - \varepsilon$. Because of the non-signaling condition, the entries for $P(ab|01)$ and $P(ab|10)$ for all $a \in A,\ b \in B$ are given:

X \ Y		0		1	
	B / A	0	1	0	1
0	0	$\frac{1}{2}+\varepsilon$	0	$\frac{1}{2}+\varepsilon$	0
	1	0	$\frac{1}{2}-\varepsilon$	0	$\frac{1}{2}-\varepsilon$
1	0	$\frac{1}{2}+\varepsilon$	0	0	$\square$
	1	0	$\frac{1}{2}-\varepsilon$	$\square$	0

(15)

It is easy to see that for any $\varepsilon \neq 0$ this box gets signaling which means that Eve can not, because of the non-signaling condition, bias a box with the behavior of a PR box. So in the case of a PR box where $(x,y) \neq (1,1)$ Alice and Bob directly share a secret bit $a = b$, and in the case where $(x,y) = (1,1)$ Bob simply takes the inverse of his output, resulting in a shared secret bit $a = \overline{b}$.

5.2 Magic Square Game and PR Box

We can win the magic square game with a single use of an NL box. In order to see this, lets assume that Alice and Bob decide on two strategies each, denoted by (S_A^0, S_A^1) and (S_B^0, S_B^1), which may look like the following:

$$S_A^0 = \begin{matrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{matrix} \qquad S_A^1 = \begin{matrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{matrix}$$

$$S_B^0 = \begin{matrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{matrix} \qquad S_B^1 = \begin{matrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{matrix}$$

Upon receiving input $x \in \{1,2,3\}$ ($y \in \{1,2,3\}$), Alice's (Bob's) input into the NL box is 0 if $x \in \{1,2\}$ ($y \in \{1,2\}$) and 1 otherwise. Alice and Bob then choose their strategies according to the output of the NL box, e.g Alice will take strategy S_A^0 if she gets output 0, and S_A^1 otherwise.
It is easy to see that all the strategies preserve the parity condition of the game and that Alice and Bob indeed will always succeed in winning. By randomizing over the different possible strategies (S_A^0, S_A^1) and (S_B^0, S_B^1), we can get the randomized statistics we may want to have.

6 Non-Signaling Attacks

In this section we want to describe an adversary's (from now on called Eve) possibilities of an attack. We want to give her as much power as possible, putting her in charge of providing physical systems or boxes to Alice and Bob, only constrained to be non-signaling. According to [4] this leads us to a three-partite scenario with an additional input-output pair (z, e) with $z \in Z$ and $e \in E$ for Eve, resulting in a probability distribution $P(abe|xyz)$. It is important to note that because of the non-signaling condition it must hold that $P(ab|xyz) = P(ab|xy)$ which means that the probability distribution of Alice and Bob does not depend on Eve's input.

Definition 6.1. *[4] A valid box partition of a given box $P_{AB|XY}$ is a family of pairs $(p_{E|Z}, P_{AB|XYZE})$, where $p_{E|Z}$ is a weight and $P_{AB|XYZE}$ is a box such that*

$$P_{AB|XY} = \sum_e p(e|z) P_{AB|XY,Z=z,E=e} \tag{16}$$

We can say that Eve's measurement result e tells her which part of the decomposition occurred. As an example consider the following non-signaling box as depicted in (17) and let $p(0|z) = \frac{2}{3}$ and $p(1|z) = \frac{1}{3}$, for some $z \in Z$.

$P_{AB|XY} =$

X \ Y		0			1		
	B / A	0	1	2	0	1	2
0	0	$\frac{1}{3}$	0	0	$\frac{1}{3}$	0	0
	1	0	$\frac{1}{3}$	0	0	$\frac{1}{3}$	0
	2	0	$\frac{1}{3}$	0	0	$\frac{1}{3}$	0
1	0	$\frac{1}{3}$	0	0	0	$\frac{1}{3}$	0
	1	0	$\frac{1}{3}$	0	$\frac{1}{3}$	0	0
	2	0	$\frac{1}{3}$	0	0	$\frac{1}{3}$	0

(17)

With $P_{AB|XY,Z=z,E=0} =$

X \ Y		0			1		
	B / A	0	1	2	0	1	2
0	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$	0	0
	1	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$	0
	2	0	0	0	0	0	0
1	0	$\frac{1}{2}$	0	0	0	$\frac{1}{2}$	0
	1	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0
	2	0	0	0	0	0	0

(18)

and $P_{AB|XY,Z=z,E=1} =$

X \ Y		0			1		
	B / A	0	1	2	0	1	2
0	0	0	0	0	0	0	0
	1	0	0	0	0	0	0
	2	0	1	0	0	1	0
1	0	0	0	0	0	0	0
	1	0	0	0	0	0	0
	2	0	1	0	0	1	0

(19)

we can write equation (16) as follows:

$$P_{AB|XY} = \frac{2}{3} P_{AB|XY,Z=z,E=0} + \frac{1}{3} P_{AB|XY,Z=z,E=1}. \tag{20}$$

We can see that in about a third of the cases Alice and Bob are using a completely local box, which, after the publication of the input, leads to perfect knowledge of Eve about the shared bit.

7 A No Signalling and Quantum Key Distribution Protocol

Barrett, Hardy and Kent [1] developed a quantum key distribution scheme provably secure against general attacks by an eavesdropper who is limited only by the impossibility of superluminal signalling. The protocol has two parameters M and N, as well as the bases

$$X_r = \{cos\frac{r\pi}{2N}|0\rangle + sin\frac{r\pi}{2N}|1\rangle, -sin\frac{r\pi}{2N}|0\rangle + cos\frac{r\pi}{2N}|1\rangle\}, \tag{21}$$

for each outcomes 0 and 1 defined by projections onto the first and second basis elements, respectively. For $r \in \{0, 1, ..., N-1\}$ they define X_{-1} and X_N to be X_{N-1} and X_0 with outcomes reversed. Alice and Bob share $n = MN^2$ pairs of systems

$$|\psi_-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{22}$$

choose random $r_A^i, r_B^i \in \{0, 1, ..., N-1\}$ for $i = 1, ...n$ and measure their i-th particle in the base $A_i := X_{r_A^i}$ and $B_i := X_{r_B^i}$. In a next step, they announce all their bases chosen and restart the protocol unless the number of neighboring or identical bases is greater or equal $2MN$. They then choose one neighboring or identical pair where Alice uses base X_i and Bob uses base $X_{i\pm1}$ and announce the measurement results of all the other pairs. If their outcomes a and b are not anti-correlated in all the cases where they chose neighboring or identical bases, Alice an Bob abort the protocol. If the protocol is not aborted, their unannounced outcomes defined the secret bit.
Obviously, it is possible that Alice and Bob do get different measurement results for a given neighboring or identical pair. In the security analysis of the protocol they derive the following lower and an upper bound for t_s being the probability that Alice and Bob end up on a different secret bit

$$1 - \frac{\delta\delta'}{3N} \geq t_s > 1 - \frac{1}{2MN\epsilon} \ , \tag{23}$$

δ' being Eve's advantage and ϵ being a lower bound for the probability of Alice and Bob not aborting the protocol during one of the test steps. *Equation 23* can be rewritten as

$$\delta\delta' < \frac{3}{2M\epsilon} \tag{24}$$

which implies that the key agreement scheme can be made arbitrarily secure by taking a large M.

7.1 Discussion

Let us now investigate the case where we have a cheating Eve. In order to have advantage d' to be $\frac{1}{2}$ she could send one system being completely local, leaving the rest unchanged. The chance that this system does not get checked is $\frac{1}{MN^2}$. The chance that her local system gets tested is $(1 - \frac{1}{MN^2})$ and the chance that this test is passed, namely that the local system has opposite measurement values is at most $1 - \frac{2}{3N}$. This means that the probability that Eve does not get caught in the case she is cheating is

$$P_{not-caught|\psi_-} \leq \frac{1}{MN^2} + (1 - \frac{1}{MN^2}) \cdot (1 - \frac{2}{3N}). \tag{25}$$

By setting the number of systems $n = MN^2$ we can rewrite the inequality to

$$\begin{aligned} P_{not-caught|\psi_-} &\leq \frac{1}{n} + (1 - \frac{1}{n}) \cdot (1 - \frac{2}{3N}) \\ &= \frac{1}{n} + 1 - \frac{1}{n} - \frac{2}{3N} + \frac{2}{3nN} \\ &= 1 - \frac{2}{3N} + \frac{2}{3nN} \end{aligned}$$

Let us now assume that instead of the states $|\psi_-\rangle$ we would take boxes used for the magic square game (MSG), where we have three input values, hence $N = 3$. Let us now compute $P_{not-caught|MSG}$ for this scenario, n again being the number of systems. The chance that the local system does again not get checked is $\frac{1}{n}$, hence the chance that her system gets checked is $1 - \frac{1}{n}$. For the

case the local system is checked we have, as each local strategy has a constant chance of winning, a probability of getting caught of $\frac{k}{N^2}$, which is equal to $\frac{1}{9}$ in the case of the magic square game. This means that we can write

$$\begin{aligned} P_{not-caught|MSG} &= \frac{1}{n} + (1 - \frac{1}{n}) \cdot (1 - \frac{k}{N^2}) \\ &= \frac{1}{n} + 1 - \frac{1}{n} - \frac{k}{N^2} + \frac{k}{nN^2} \\ &= 1 - \frac{k}{N^2} + \frac{k}{nN^2} \end{aligned}$$

It turns out that there are better chances to get through cheating in the case of using magic square game boxes. When using those boxes, we have the probability to get caught:

$$\begin{aligned} P_{caught|MSG} &= 1 - P_{not-caught|MSG} \\ &= \frac{k}{N^2} - \frac{k}{nN^2} \\ &= \frac{k}{N^2} \cdot (1 - \frac{1}{n}) \end{aligned}$$

For the $|\psi_-\rangle$ boxes we have

$$\begin{aligned} P_{caught|\psi_-} &= 1 - P_{not-caught|\psi_-} \\ &= \frac{2}{3N} - \frac{2}{3nN} \\ &= \frac{2}{3N} \cdot (1 - \frac{1}{n}). \end{aligned}$$

This implies that in the case of using $|\psi_-\rangle$ boxes, the more bases we chose, the smaller the probability of catching a cheater gets. Let us now consider the case where there is no cheating Eve. In the case of $|\psi_-\rangle$ being shared we have that the probability of Alice and Bob not choosing enough neighboring or identical bases is of order $e^{-\frac{MN}{6}}$ and hence the probability of passing that test is of order $1 - e^{-\frac{MN}{6}}$. The expected sum of identical or neighboring bases is $3MN$ so the expected sum of neighboring bases is $2MN$. The probability that Alice and Bob get different measurement results, given that they measure in neighboring bases is $cos^2(\frac{\pi}{2N})$. This leads us to

$$P_{succ|no-eve,\psi_-} = (1 - e^{-\frac{MN}{6}}) \cdot (cos^2(\frac{\pi}{2N}))^{2MN} \quad (26)$$

$$= (1 - e^{-\frac{MN}{6}}) \cdot (1 - sin^2(\frac{\pi}{2N}))^{2MN} \quad (27)$$

$$\approx (1 - e^{-\frac{MN}{6}}) \cdot (1 - \frac{\pi^2}{4N^2})^{2MN} \quad (28)$$

For the case where we use magic square boxes, we obviously have

$$P_{succ|no-eve,MSG} = 1. \quad (29)$$

In terms of completeness, it seems to be a good idea to use quantum pseudo telepathy game boxes, as, if everyone is honest, Alice and Bob would always succeed in generating a perfectly secure, shared bit. In fact, for the usage of $|\psi_-\rangle$ boxes there is a tradeoff: The better you want to be able to catch a cheater, the less bases you got to chose, which, on the other hand, lowers the probability of succeeding in the case everybody playing correctly.

8 Box Transformation

Consider the following scenario: Alice and Bob share a non-signalling box with input sets (X,Y) and output sets (A,B). In each round, Alice chooses an element $x \in X$ and Bob $y \in Y$ randomly, used as input for the box. Note that these inputs are made public, as described in *Section 4*. Upon receiving their output they are now allowed to apply operations to their input-output pairs which consist of the following:

Definition 8.1. *The set of possible local operations:*

1. *Discard or aggregation of input.*
2. *Discard or aggregation of output depending on the input.*
3. *Permutation of output depending on the input.*

Definition 8.2. *A box $P(ab|xy)$ can be locally transformed to a PR box $P_{PR}(ab|xy)$, denoted as $P(ab|xy) \succ_l P_{PR}(ab|xy)$, if, by applying operations from definition 8.1, one gets an input-output statistics of a PR box.*

Example 8.3. *A possible, non-signalling box shared by Alice and Bob is depicted in (17) and has $X = Y = \{0, 1\}$ and $A = B = \{0, 1, 2\}$. It is easy to see that if Alice drops all the pairs (x_i, a_i) with $a_i = 2$ and Bob drops all the pairs (y_i, b_i) with $b_i = 2$, they transform the box to a PR box as shown in (10).*

Example 8.4. *If we take*

X \ Y		0			1		
	B / A	0	1	2	0	1	2
0	0	p	0	0	p	0	0
	1	0	p	0	0	p	0
	2	0	0	p	0	0	p
1	0	p	0	0	0	p	0
	1	0	p	0	0	0	p
	2	0	0	p	p	0	0

(30)

Bob can apply the following permutation (Operation 3) on his output b in the case of input $x = y = 1$: $\{0 \to 2, 1 \to 1, 2 \to 0\}$, which would result in

X \ Y		0			1		
	B / A	0	1	2	0	1	2
0	0	p	0	0	p	0	0
	1	0	p	0	0	p	0
	2	0	0	p	0	0	p
1	0	p	0	0	0	p	0
	1	0	p	0	p	0	0
	2	0	0	p	0	0	p

(31)

It is easy to see that if Alice and Bob share a box as in (31) and if (like in example 8.3) Alice drops all the pairs (x_i, a_i) with $a_i = 2$ and Bob drops all the pairs (y_i, b_i) with $b_i = 2$, they transform the box to a PR box as shown in (10).

9 Requirements for a Perfectly Secret Bit

In association with perfectly secret and shared bits there are two requirements which have to be fulfilled. First, we need correctness, meaning that the output used for bit agreement needs to be either perfectly correlated or anti-correlated. On the other hand, we also need secrecy, preventing any attacker from successfully biasing the shared bit.

Definition 9.1. *Let $P_{local-det}$ be a local deterministic box. It has the property that for any input pair (x, y) there is only one output pair (a, b) with $P_{local-det}(ab|xy) = 1$.*

Definition 9.2. *Let $P_{PR,emb}$ be a box which can be transformed into a PR box by only discarding entries having value equal to 0. Such a box gets signaling as soon as $|X| > 2$ or $|Y| > 2$.*

Definition 9.3. *Let $P_{not-disc}$ be a box which has some perfectly correlated or perfectly anticorrelated outputs, and the rest filled up with probability zero.*

Definition 9.4. *Let P_{sec} be a non-signalling box which can be used by Alice and Bob to generate a common perfectly secret bit.*

9.1 Requirements for Systems with Input Dimension 2

In the case of binary input, the need for secrecy and correctness implies that, in order to have a perfectly secret bit for Alice and Bob, we need either a PR box with perfectly correlated output (correctness) or else a non-local box, from which we could extract a PR box by deleting input and output, as described in *Section 8.* From now on, the part of a probability distribution $P(ab|xy)$ getting discarded is denoted by $P_{disc}(ab|xy)$. Additionally, we need to make sure that Eve fails to perform a box partition attack (secrecy) *(Section 6).* This implies that Eve's only possibilities of partitioning must be in such a way that the PR part remains unchanged (i.e. that it does not split into different parts) and that the whole local rest corresponds to the part being discarded by Alice and Bob. Let us call such boxes, which allow Alice and Bob to have perfect secrecy $P_{succ}(ab|xy)$.

Lemma 9.5. *A probability distribution $P(ab|xy)$ with $|X| = |Y| = 2$ can be used to generate a shared, perfectly secret bit, if it can be written as*

$$P = P_{PR,emb} + P_{disc} \tag{32}$$

and if the following holds: For any $P_{local-det}$ and

$$T = P - P_{local-det} \tag{33}$$

where exists a tuple (a, b, x, y) for which holds that

$$(P_{local-det}(ab|xy) = 1) \wedge (P_{PR,emb}(ab|xy) \neq 0), \tag{34}$$

we have

$$\exists(a', b', x', y') : T(a'b'|x'y') = -1. \tag{35}$$

Proof: Assume we have a non-local probability distribution

$$P = P_{PR,emb} + P_{disc}$$

which is vulnerable to a non-signaling box partition attack. This implies that there must exist a valid partitioning

$$P = (1 - w_{local-det})P_{non-signalling} + w_{local-det}P_{local-det}$$

such that

$$\exists(a,b,x,y): \ (P_{local-det}(ab|xy) = 1) \wedge (P_{PR,emb}(ab|xy) \neq 0).$$

This and the fact that P is non-signalling implies

$$\forall(a,b,x,y): \ P(ab|xy) - P_{local}(ab|xy) > -1.$$

□

Example 9.6. *The following box*

$P =$

		0			1		
		0	1	2	0	1	2
0	0	$\frac{2}{5}$	0	0	$\frac{2}{5}$	0	0
	1	0	$\frac{2}{5}$	0	0	$\frac{2}{5}$	0
	2	0	$\frac{1}{5}$	0	0	$\frac{1}{5}$	0
1	0	$\frac{2}{5}$	0	0	0	$\frac{2}{5}$	0
	1	0	$\frac{2}{5}$	0	$\frac{2}{5}$	0	0
	2	0	$\frac{1}{5}$	0	0	$\frac{1}{5}$	0

(36)

can be written as (32) with

$$\begin{aligned} P_{PR,emb} &:= P(ab|xy), \ a < 2, \ b < 2, \ x,y \in \{0,1\} \\ P_{disc} &:= P(ab|xy), \ a = b = 2, \ x,y \in \{0,1\} \end{aligned}$$

Now lets consider a grid $P_{local-det}$ with entries where indicated in P by the lightgray shades. This grid fulfills (34) but violates (35). For the sake of completeness, a possible partition attack is given: $P =$

$\frac{4}{5} \cdot$

		0			1		
		0	1	2	0	1	2
0	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$	0	0
	1	0	$\frac{1}{4}$	0	0	$\frac{1}{4}$	0
	2	0	$\frac{1}{4}$	0	0	$\frac{1}{4}$	0
1	0	$\frac{1}{2}$	0	0	0	$\frac{1}{2}$	0
	1	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0
	2	0	0	0	0	0	0

$+ \ \frac{1}{5} \cdot$

		0			1		
		0	1	2	0	1	2
0	0	0	0	0	0	0	0
	1	0	1	0	0	1	0
	2	0	0	0	0	0	0
1	0	0	0	0	0	0	0
	1	0	0	0	0	0	0
	2	0	1	0	0	1	0

resulting in a winning probability of $\frac{1}{5} \cdot \frac{1}{2} = \frac{1}{10}$ *for Eve.*

Example 9.7. *The following box*

$$P \;=\; \begin{array}{cc|ccc||ccc} & & \multicolumn{3}{c||}{0} & \multicolumn{3}{c}{1} \\ & & 0 & 1 & 2 & 0 & 1 & 2 \\ \hline\hline 0 & 0 & \frac{1}{9} & 0 & 0 & \frac{1}{9} & 0 & 0 \\ & 1 & 0 & \frac{1}{9} & 0 & 0 & \frac{1}{9} & 0 \\ & 2 & \frac{2}{9} & \frac{2}{9} & \frac{3}{9} & \frac{2}{9} & \frac{2}{9} & \frac{3}{9} \\ \hline 1 & 0 & \frac{1}{9} & 0 & 0 & 0 & \frac{1}{9} & 0 \\ & 1 & 0 & \frac{1}{9} & 0 & \frac{1}{9} & 0 & 0 \\ & 2 & \frac{2}{9} & \frac{2}{9} & \frac{3}{9} & \frac{2}{9} & \frac{2}{9} & \frac{3}{9} \end{array} \tag{37}$$

can be written as (32) with

$$\begin{aligned} P_{PR,emb} &:= P(ab|xy),\ a<2,\ b<2,\ x,y\in\{0,1\} \\ P_{disc} &:= P(ab|xy),\ a=b=2,\ x,y\in\{0,1\} \end{aligned}$$

Now lets consider a grid $P_{local-det}$ with entries where indicated in P by the lightgray shades. This grid fulfills (34) and but violates (35). For the sake of completeness, a possible partition attack is given: $P =$

$$\frac{8}{9}\cdot \begin{array}{cc|ccc||ccc} & & \multicolumn{3}{c||}{0} & \multicolumn{3}{c}{1} \\ & & 0 & 1 & 2 & 0 & 1 & 2 \\ \hline\hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & \frac{1}{8} & 0 & 0 & \frac{1}{8} & 0 \\ & 2 & \frac{2}{8} & \frac{2}{8} & \frac{3}{8} & \frac{2}{8} & \frac{2}{8} & \frac{3}{8} \\ \hline 1 & 0 & \frac{1}{8} & 0 & 0 & 0 & \frac{1}{8} & 0 \\ & 1 & 0 & \frac{1}{8} & 0 & \frac{1}{8} & 0 & 0 \\ & 2 & \frac{1}{8} & \frac{2}{8} & \frac{3}{8} & \frac{1}{8} & \frac{2}{8} & \frac{3}{8} \end{array} + \frac{1}{9}\cdot \begin{array}{cc|ccc||ccc} & & \multicolumn{3}{c||}{0} & \multicolumn{3}{c}{1} \\ & & 0 & 1 & 2 & 0 & 1 & 2 \\ \hline\hline 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ & 2 & 1 & 0 & 0 & 1 & 0 & 0 \end{array}$$

resulting in a winning probability of $\frac{1}{9}\cdot\frac{1}{2}=\frac{1}{18}$ for Eve.

Example 9.8. *The following box*

$$P \;=\; \begin{array}{cc|ccc||ccc} & & \multicolumn{3}{c||}{0} & \multicolumn{3}{c}{1} \\ & & 0 & 1 & 2 & 0 & 1 & 2 \\ \hline\hline 0 & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & 0 \\ & 1 & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 \\ & 2 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} \\ \hline 1 & 0 & \frac{1}{4} & 0 & 0 & 0 & \frac{1}{4} & 0 \\ & 1 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 \\ & 2 & \frac{1}{2} & 0 & 0 & 0 & 0 & \frac{1}{2} \end{array} \tag{38}$$

can be written as (32) with

$$\begin{aligned} P_{PR,emb} &:= P(ab|xy),\ a<2,\ b<2,\ x,y\in\{0,1\} \\ P_{disc} &:= P(ab|xy),\ a=b=2,\ x,y\in\{0,1\} \end{aligned}$$

A possible grid $P_{local-det}$ for example with entries where indicated in P by the lightgray shades fulfills (34). It is easy to see that P also meets (35) as $P(20|11)$ has value 0. To see that this applies to any possible grid fullfilling (34) is tedious but straightforward.

9.2 Requirements for Systems with Higher Input Dimension

9.2.1 The case of binary output

As we already know, the most general way to build a probability distribution P for secret bits is such that it prohibits any kind of box partition attack. Due to privacy, the entries which do not get discarded, $P_{not-disc}$, need to be either perfectly correlated or perfectly anti-correlated. Please note that both P_{disc} and $P_{not-disc}$ may be signaling. As a motivating example let us look at the following probability distribution:

Example 9.9.

$P =$

		0		1		2		3		4	
		0	1	0	1	0	1	0	1	0	1
0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	□	□	□	□	0	$\frac{1}{2}$
	1	0	$\frac{1}{2}$	0	$\frac{1}{2}$	□	□	□	□	$\frac{1}{2}$	0
1	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	□	□	□	□
	1	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	□	□	□	□
2	0	□	□	$\frac{1}{2}$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	□	□
	1	□	□	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	□	□
3	0	□	□	□	□	$\frac{1}{2}$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0
	1	□	□	□	□	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	$\frac{1}{2}$
4	0	0	$\frac{1}{2}$	□	□	□	□	$\frac{1}{2}$	0	$\frac{1}{2}$	0
	1	$\frac{1}{2}$	0	□	□	□	□	0	$\frac{1}{2}$	0	$\frac{1}{2}$

(39)

Note that the tiny boxes indicate any values that complement the box to a non-signaling probability distribution. The box only containing those box-values is denoted as P_{disc} and the rest as $P_{not-disc}$. Although this box can not be transformed into a PR box, Alice and Bob are able to generate a perfectly secret bit (see next) by discarding all the input entries indicated by those tiny boxes.

We now want to characterize a probability distribution P for the case of binary output.

Lemma 9.10. *A probability distribution P with $|A| = |B| = 2$, $|X| = m$ and $|Y| = n$ can be used to generate a shared, perfectly secret bit, if it can be written as*

$$\begin{aligned} P &= P_{not-disc} + wP_{disc} \\ w &\in \{0,1\} \end{aligned} \tag{40}$$

and if the following holds: For any $P_{local-det}$ and

$$T = P - P_{local-det} \tag{41}$$

we have

$$\exists (a,b,x,y) : T(ab|xy) = -1. \tag{42}$$

Obviously, w must be equal to 1 if $P_{not-disc} \not\prec_l PR$.
Proof: Assume we have a non-local probability distribution

$$P = P_{not-disc} + P_{disc}$$

which is vulnerable to a non-signaling box partition attack. This implies that there must be a valid partitioning like

$$P = (1 - w_{local})P_{non-signalling} + w_{local}P_{local}. \tag{43}$$

This implies further that P_{local} enables a $P_{local-det}$ as in (41). Because of the non-signaling condition we finally have that

$$\forall(a, b, x, y) : \ P(ab|xy) - P_{local}(ab|xy) > -1.$$

□

As a special case it is easy to see that if $P_{not-disc}$ can be transformed into a PR box, the lemma is trivially true.

Example 9.11. *Lets consider the following box P with $|X| = |Y| = 3$ and $|A| = |B| = 2$:*

$P =$

		0		1		2	
		0	1	0	1	0	1
0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	□	□
	1	0	$\frac{1}{2}$	0	$\frac{1}{2}$	□	□
1	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$	□	□
	1	0	$\frac{1}{2}$	$\frac{1}{2}$	0	□	□
2	0	□	□	□	□	□	□
	1	□	□	□	□	□	□

(44)

We can write

$$\begin{aligned} P &= P_{disc} + P_{not-disc} \text{ with} \\ P_{disc} &= P(ab|22), a \in A, \ b \in B, \\ P_{not-disc} &= P(ab|x < 2, y < 2), \ x < 2, \ y < 2, \end{aligned}$$

$P_{not-disc}$ being a PR box. It is easy to see that all possible $P_{local-det}$ (e.g. the one indicated by the lightgray shade), when subtracted from $P_{not-disc}$ would result in an entry equal to -1 (e.g. for $P(00|11)$).

Example 9.12. *Lets consider the following box P:*

$P =$

		0		1		2	
		0	1	0	1	0	1
0	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0
	1	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$
1	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0
	1	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$
2	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$	□	□
	1	0	$\frac{1}{2}$	$\frac{1}{2}$	0	□	□

(45)

If we put a perfect anti-correlation distribution into the tiny boxes, we would have a PR box for $x, y \in \{1, 2\}$ and hence a box for perfectly secret bits, but if we insert a perfect correlation distribution, the whole box would become local as indicated by the lightgray shaded entries.

9.3 The General Case

In this subsection we want to generalize the requirements for secret bits for boxes with arbitrary input and output dimension.

Lemma 9.13. *A probability distribution P can be used to generate a shared, perfectly secret bit, if it can be written as*

$$P = P_{not-disc} + P_{disc} \tag{46}$$

and if the following holds: If for any $P_{local-det}$ and

$$T = P - P_{local-det} \tag{47}$$

there exists a tuple (a, b, x, y) for which holds that

$$(P_{local-det}(ab|xy) = 1) \wedge (P_{not-disc}(ab|xy) \neq 0), \tag{48}$$

we have that

$$\exists(a', b', x', y') : T(a'b'|x'y') = -1. \tag{49}$$

Proof: Assume we have a box P for which exists a $P_{local-det}$ with a tuple (a, b, x, y) fulfilling (48). Further assume that each entry of $T = P - P_{local-det}$ is greater that -1. This directly leads us to a possible partition attack, namely the $P_{local-det}$.

□

10 Perfect Security and Feasibility

In *Section 9* we dealt with probability distributions or boxes and analyzed their structure needed in order to generate perfectly secret bits. Obviously, what we are now interested in is whether such boxes can be implemented by the means of quantum mechanics or not. Navascues, Pironio and Acin [6] introduced a hierarchy of conditions which need to be satisfied by any box P resulting from two separate observers locally measuring on shared quantum states with outcomes $a \in A$ and $b \in B$.
They state that a box $P_{\alpha\beta}$ admits a quantum representation if there exists a joint quantum state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ and two sets of projection operators, namely $E_\alpha = \tilde{E_\alpha} \otimes I$ acting on Alice's system and $E_\beta = I \otimes \tilde{E_\beta}$ acting on Bob's system, such that $P_{\alpha\beta} = tr(E_\alpha E_\beta \rho)$. Projectors belonging to the same measurement should be pairwise orthogonal and sum to the identity. For example, let A_0^1 be a projector of Alice's which states that measurement, or input, is 1 and result, or output, is 0. On the first level of the hierarchy they use the set of all single projectors including the identity operator, like for example in the case of binary input and binary output $S = \{1, A_0^0, A_0^1, A_1^0, A_1^1, B_0^0, B_0^1, B_1^0, B_1^1\}$, in order to build the matrix Γ where

$$\Gamma_{i,j} = tr(S_i^\dagger S_j \rho). \tag{50}$$

So as an example $tr(A_0^{0\dagger}B_0^1\rho)$ would correspond to the probability $P(00|01)$. Note that an entry like $tr(A_1^{0\dagger}A_1^1\rho)$ is not valid which is why a variable is put in place there. They state that for every box, in order to be implementable by the means of quantum mechanics, the variables of the matrix Γ constructed from this box must have an assignment making the whole matrix positive semidefinite, namely $\Gamma \succeq 0$.

10.1 The Case of Binary Input and Binary Output

In order to start with the case of binary input and binary output, let us investigate the PR box. According to the previous section, the matrix looks as follows:

$$\Gamma' = \begin{array}{c|ccccccccc} & 1 & A_0^0 & A_1^0 & A_0^1 & A_1^1 & B_0^0 & B_1^0 & B_0^1 & B_1^1 \\ \hline 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ A_0^0 & \frac{1}{2} & \frac{1}{2} & u & v & w & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ A_1^0 & \frac{1}{2} & u & \frac{1}{2} & v' & w' & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ A_0^1 & \frac{1}{2} & v & v' & \frac{1}{2} & w'' & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ A_1^1 & \frac{1}{2} & w & w' & w'' & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ B_0^0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & u''' & v''' & w''' \\ B_1^0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & \frac{1}{2} & u''' & \frac{1}{2} & v'''' & w'''' \\ B_0^1 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & \frac{1}{2} & v''' & v'''' & \frac{1}{2} & w''''' \\ B_1^1 & \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & w''' & w'''' & w''''' & \frac{1}{2} \end{array} \tag{51}$$

As $A_0^0 = 1 - A_1^0$, $A_0^1 = 1 - A_1^1$, $B_0^0 = 1 - B_1^0$ and $B_0^1 = 1 - B_1^1$, we can write

$$\Gamma = \begin{array}{c|ccccc} & 1 & A_0^0 & A_0^1 & B_0^0 & B_0^1 \\ \hline 1 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ A_0^0 & \frac{1}{2} & \frac{1}{2} & u & \frac{1}{2} & \frac{1}{2} \\ A_0^1 & \frac{1}{2} & u & \frac{1}{2} & \frac{1}{2} & 0 \\ B_0^0 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & v \\ B_0^1 & \frac{1}{2} & \frac{1}{2} & 0 & v & \frac{1}{2} \end{array} \tag{52}$$

In order to be positive semidefinite, all minors of Γ, e.g. the following ones, have to be greater or equal to zero:

$$\Gamma_{PR} = u^2v^2 + \frac{1}{4}uv - \frac{1}{2}uv^2 - \frac{1}{2}u^2v \tag{53}$$

$$\Gamma_{2,3,4,5} = -\frac{1}{4}v^2 - \frac{1}{4}u^2 + u^2v^2 + \frac{1}{4}u - \frac{1}{2}uv - \frac{1}{16} + \frac{1}{4}v \tag{54}$$

$$\Gamma_{3,4,5} = -\frac{1}{2}v^2 \tag{55}$$

$$\Gamma_{4,5} = \frac{1}{4} - v^2 \tag{56}$$

$$\Gamma_5 = \frac{1}{2} \tag{57}$$

$$\Gamma_{2,3,5} = -\frac{1}{2}u^2 \tag{58}$$

Since $-\frac{1}{2}v^2 \stackrel{!}{\geq} 0$ (55) we have $v \stackrel{!}{=} 0$ and since $-\frac{1}{2}u^2 \stackrel{!}{\geq} 0$ (58) we have $u \stackrel{!}{=} 0$. The substitution into $\Gamma_{2,3,4,5}$ gives us

$$\Gamma_{2,3,4,5} = -\frac{1}{16} \; < \; 0$$

which means that Γ is not positive semidefinite and, as we already knew, that the PR box has no physical representation in the quantum world.

Lemma 10.1. *Any probability distribution P with $|A| = |B| = 2$ which can be reduced to a PR box results in a matrix Γ which is not positive semidefinite, which implies further that $P(ab|xy)$ is not implementable by the means of quantum mechanics.*

Proof: Let us consider the construction of the matrix Γ for a P containing a PR box. Without loss of generality, let A^x, $A^{x'}$, B^y and $B^{y'}$ be the four input values with the output statistics of a PR. This means that we can directly extract the minor Γ_{PR} corresponding to the probabilities for those four values. From above we know that Γ_{PR} is not positive semidefinite which means that Γ is not, neither.

□

Lemma 10.2. *The following box*

$$P \;=\; \begin{array}{|cc||c|c||c|c|}\hline & & \multicolumn{2}{c||}{0} & \multicolumn{2}{c|}{1} \\ & & 0 & 1 & 0 & 1 \\ \hline\hline 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ \cline{2-6} & 1 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \hline\hline 1 & 0 & \frac{1}{2} & 0 & p & \varepsilon \\ \cline{2-6} & 1 & 0 & \frac{1}{2} & \varepsilon & p \\ \hline\hline \end{array} \tag{59}$$

with

$$p \;=\; \frac{1}{2} - \varepsilon \tag{60}$$

$$\varepsilon \;>\; 0 \tag{61}$$

can not be implemented by the means of quantum mechanics.

Proof: Again, let's consider the Γ matrix:

$$\Gamma \;=\; \begin{array}{c|ccccc} & 1 & A_0^0 & A_0^1 & B_0^0 & B_0^1 \\ \hline 1 & 1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ A_0^0 & \frac{1}{2} & \frac{1}{2} & u & \frac{1}{2} & \frac{1}{2} \\ A_0^1 & \frac{1}{2} & u & \frac{1}{2} & \frac{1}{2} & p \\ B_0^0 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & v \\ B_0^1 & \frac{1}{2} & \frac{1}{2} & p & v & \frac{1}{2} \end{array} \tag{62}$$

The following minors have again to be greater or equal to zero in order for Γ to be positive semidefinite.

$$\begin{aligned}
\Gamma &= \frac{1}{4}pv + u^2v^2 - \frac{1}{2}upv + \frac{1}{4}up - \frac{1}{8}p - \frac{1}{2}uv^2 - \frac{1}{2}u^2v + \frac{1}{4}uv \\
\Gamma_{2,3,4,5} &= -\frac{1}{4}v^2 + \frac{1}{2}pv - \frac{1}{4}u^2 + u^2v^2 + \frac{1}{4}u - \frac{1}{2}uv - upv + \frac{1}{2}up - \frac{1}{16} + \frac{1}{4}v - \frac{1}{4}p \\
\Gamma_{3,4,5} &= -\frac{1}{2}v^2 + pv - \frac{1}{2}p^2 \\
\Gamma_{4,5} &= \frac{1}{4} - v^2 \\
\Gamma_{2,3,5} &= -\frac{1}{2}p^2 - \frac{1}{2}u^2 + up \\
\Gamma_{1,2,3} &= -u^2 + \frac{1}{2}u \\
\Gamma_{2,3} &= \frac{1}{4} - u^2 \\
\Gamma_{3,5} &= \frac{1}{4} - p^2
\end{aligned}$$

From $\Gamma_{4,5}$, $\Gamma_{2,3}$ and $\Gamma_{3,5}$ we have

$$\begin{aligned}
-\frac{1}{2} \leq v \leq \frac{1}{2} \\
-\frac{1}{2} \leq u \leq \frac{1}{2} \\
-\frac{1}{2} \leq p \leq \frac{1}{2}.
\end{aligned} \tag{63}$$

From $\Gamma_{2,3,5}$ we have

$$\begin{aligned}
-\frac{1}{2}p^2 - \frac{1}{2}u^2 + up &\geq 0 \Leftrightarrow \\
-(p^2 + u^2 - 2up) &\geq 0 \Leftrightarrow \\
-(p-u)^2 &\geq 0 \Leftrightarrow \\
p &= u.
\end{aligned}$$

and $\Gamma_{3,4,5}$ gives us

$$\begin{aligned}
-\frac{1}{2}v^2 + pv - \frac{1}{2}p^2 &\geq 0 \Leftrightarrow \\
-(v^2 - 2pv + p^2) &\geq 0 \Leftrightarrow \\
-(v-p)^2 &\geq 0 \Leftrightarrow \\
v &= p.
\end{aligned}$$

This means that we have $u = v = p$. Substituted into $\Gamma_{2,3,4,5}$ we get

$$\Gamma_{2,3,4,5} = p^4 + \frac{1}{4}p - p^3 - \frac{1}{16} \tag{64}$$

$p^4 + \frac{1}{4}p - p^3 - \frac{1}{16} \geq 0$ (64) has the following solution:

$$\begin{aligned}
p &\leq -\frac{1}{2} \\
p &\geq \frac{1}{2}
\end{aligned}$$

Combined with Equation 63 we get

$$\begin{aligned} p_1 &= -\frac{1}{2} \\ p_2 &= \frac{1}{2} \end{aligned}$$

We can skip p_1 as we do not have negative probabilities in a box. If we look at Equation 60 we see that $p = p_1 = \frac{1}{2}$ requires $\varepsilon = 0$ which leads to a contradiction in Equation 61.

□

We can show the same way that every box P with $|A| = |B| = |X| = |Y| = 2$ with three times perfect correlation or anticorrelation as in 65

$$\begin{array}{|c|c|}\hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array}\ , \quad \begin{array}{|c|c|}\hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array} \tag{65}$$

can not be implemented if the fourth output pair is of the following form with $\varepsilon > 0$

$$\begin{array}{|c|c|}\hline \frac{1}{2} - \varepsilon & \varepsilon \\ \hline \varepsilon & \frac{1}{2} - \varepsilon \\ \hline \end{array}\ . \tag{66}$$

Lemma 10.3. *Every box P with binary output, containing a box as 62 can not be implemented by the means of quantum mechanics.*

Again, by construction, the matrix Γ of a box P containing a box as 62 contains a minor directly corresponding to 62. This implies that such a Γ is not positive semidefinite.

10.2 The Case of Binary Output and More Input

In *Lemma 9.10* we learned that subtracting any possible local deterministic strategy from a P_{sec} results in an entry of minus one. We now want to work out further properties. As we know, a PR is secure and hence any P containing such a PR box is secure as well. On the other hand, we saw in *Example 9.9* that there exist P_{sec} not containing a PR box. Let us now assume we have such a

$$P_{sec} = P_{not-disc} + w_{disc} P_{disc} \tag{67}$$

$$w_{disc} \in \{0, 1\}$$

$$P_{not-disc} \not\geq_l PR \tag{68}$$

Obviously, we need w_{disc} to be equal to 1, because in the case of $w_{disc} = 0$, P_{sec} would not be secure anymore (68). We further can assume that for each entry $P(ab|xy)$ of P_{disc} there must exist

1. x', such that $\sum_{a,b} P_{not-disc}(ab|x'y) = 1$ and
2. y', such that $\sum_{a,b} P_{not-disc}(ab|xy') = 1$,

because if *1* (*2*) is violated, we can discard the corresponding column (row).

Lemma 10.4. *For a feasible box P any subbox P', comprising a subset of the inputs of P, has to be feasible as well.*

Proof: Again, using the same argument as in the sections above we can say that as soon that some subbox P' is infeasible, it's matrix $\Gamma_{P'}$ is not positive semidefinite which implies that Γ_P is not, neither.

□

We know that for every P_{succ} there does not exist a local-deterministic strategy or grid. Let P_{min} be the smallest subset of inputs of P_{succ} not admitting such a local-deterministic strategy. From above we know that on each row and on each column there must exist at least one entry containing perfect correlation or anti-correlation, so without loss of generality, let's say that for a given input x and y we have that $P_{min}(ab|xy)$ corresponds to one of those diagonal entries. Now let us have a look at x-the row of P_{min}. If there are no more diagonal entries on that row we know that this row does not contribute to the fact that there is no grid for P_{min}, which means that P_{min} is secure without that row. But as this would be a contradiction to the minimality of P_{min}, we know that there must be at least one other y' such that $P_{min}(ab|xy')$ is diagonal. Using the same argument we know that also on the y-th column there exists a x' with $P_{min}(ab|x'y)$ being diagonal. Because of the non-signaling condition, $P_{min}(ab|x'y')$ must be of the following form:

$$\begin{aligned} P_{min}(ab|x'y') &= w_c \begin{array}{|c|c|}\hline 1 & 0 \\ \hline 0 & 1 \\ \hline \end{array} + (1-w_c) \begin{array}{|c|c|}\hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array} \qquad (69) \\ w_c,\ w_a &\geq 0 \\ w_c + w_a &= \frac{1}{2} \end{aligned}$$

Case A: If $0 < w_c < 1$ we know from *Lemma 10.3* that P can not be implemented by the means of quantum mechanics.
Case B: For $x \in \{0,1\}$ let $w_c = x$ be the case of P' being a PR box. In this case we know from *Lemma 10.1* that a box as P can not exist.
Case C: In this case we know that $w_c = \overline{x}$ complements P' to a local box.

As Case A and B make the whole box infeasible, we know that we must have a Case C, which further means that again either the x'-row or the y'-th column does not help preventing a possible grid so far. Hence, the only possibility left is that there are two more diagonal entries, namely one for $P_{min}(ab|x'', y')$ and one for $P_{min}(ab|x', y'')$. Obviously, we now have new input pairs such as $P_{min}(ab|x''y')$ for which we can again conclude, using analysis of the three Cases A, B and C, that preserving feasibility enlarges the part of P_{min} being local. If we continue until all the input pairs of P_{min} have been analyzed we see that P_{min} is feasible if and only if the whole box is local which means that the box is not secure at all.

10.2.1 Conclusion

Roger Colbeck and Renato Renner [3] showed in their article that, in the case of binary output, in order to get perfectly correlated, uniformly distributed and

secure output we would need unlimited inputs. Now, we have seen that quantum mechanics does not allow us to generate a box with a finite number of inputs to produce perfectly secure, shared bits between two parties. Moreover, we've found out that perfect secrecy requires maximal non-local correlations. As we know, pseudo telepathy equips us with some perfectly correlated output, e.g. the intersection bit in case of the magic square game. Unfortunately, the only way of making perfect correlation secret is, in case of finite input, to have maximal non-locality which permits any quantum simulation. This finally means that the principle of quantum pseudo telepathy games does not help us generating perfectly secure, shared bits.

10.3 The Case of Binary Input and More Output

Let us consider the case of three outputs $A = B = \{0, 1, \delta\}$ with δ being discarded. As we know, for a common secret bit we need a PR part inside the box, which leads us to the following:

$$P = \begin{array}{|c|c||c|c|c||c|c|c|}\hline & & \multicolumn{3}{c||}{0} & \multicolumn{3}{c|}{1} \\ \hline & & 0 & 1 & \Delta & 0 & 1 & \Delta \\ \hline\hline 0 & 0 & a & 0 & \delta_1 & a & 0 & \delta_1 \\ \hline & 1 & 0 & a & \delta_2 & 0 & a & \delta_2 \\ \hline & \Delta & \delta_3 & \delta_4 & \delta_5 & \delta_8 & \delta_9 & \delta_{10} \\ \hline\hline 1 & 0 & a & 0 & \delta_6 & 0 & a & \delta_6 \\ \hline & 1 & 0 & a & \delta_7 & a & 0 & \delta_7 \\ \hline & \Delta & \delta_3 & \delta_4 & \delta_{11} & \delta_8 & \delta_9 & \delta_{12} \\ \hline\end{array} \tag{70}$$

where

$$\begin{aligned} \delta_5 &= 1 - 2a - \delta_1 - \delta_2 - \delta_3 - \delta_4 \\ \delta_{10} &= 1 - 2a - \delta_1 - \delta_2 - \delta_8 - \delta_9 \\ \delta_{11} &= 1 - 2a - \delta_3 - \delta_4 - \delta_6 - \delta_7 \\ \delta_{12} &= 1 - 2a - \delta_6 - \delta_7 - \delta_8 - \delta_9. \end{aligned}$$

If we look for example at δ_3 and δ_9 we see that if they are both greater than zero, there is the following partition attack (let $a \geq \delta_3 \geq \delta_9$ and $v = (1 - \delta_9)$).

$P =$

$$
v \cdot
\begin{array}{c|c||ccc||ccc|}
 & & \multicolumn{3}{c||}{0} & \multicolumn{3}{c|}{1} \\
 & & 0 & 1 & 2 & 0 & 1 & 2 \\
\hline\hline
0 & 0 & \frac{a}{v} & 0 & \frac{\delta_1}{v} & \frac{a}{v} & 0 & \frac{\delta_1}{v} \\
 & 1 & 0 & \frac{a}{v} & \frac{\delta_2}{v} & 0 & \frac{a}{v} & \frac{\delta_2}{v} \\
 & 2 & \frac{\delta_3-\delta_9}{v} & \frac{\delta_4-\delta_9}{v} & \frac{\delta_5-\delta_9}{v} & \frac{\delta_8-\delta_9}{v} & 0 & \frac{\delta_{10}-\delta_9}{v} \\
\hline\hline
1 & 0 & \frac{a}{v} & 0 & \frac{\delta_6}{v} & 0 & \frac{a}{v} & \frac{\delta_6}{v} \\
 & 1 & 0 & \frac{a}{v} & \frac{\delta_7}{v} & \frac{a}{v} & 0 & \frac{\delta_7}{v} \\
 & 2 & \frac{\delta_3-\delta_9}{v} & \frac{\delta_4-\delta_9}{v} & \frac{\delta_{11}-\delta_9}{v} & \frac{\delta_8-\delta_9}{v} & 0 & \frac{\delta_{12}-\delta_9}{v} \\
\hline\hline
\end{array}
$$

$$
+ \quad \delta_9 \quad \cdot
\begin{array}{c|c||ccc||ccc|}
 & & \multicolumn{3}{c||}{0} & \multicolumn{3}{c|}{1} \\
 & & 0 & 1 & 2 & 0 & 1 & 2 \\
\hline\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & 2 & 1 & 0 & 0 & 0 & 1 & 0 \\
\hline\hline
1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline\hline
\end{array}
\tag{71}
$$

Thus, in order to have a secure box, we require $\delta_3 > 0 \Rightarrow \delta_9 = 0$ and vice versa, or simply: $\delta_3 \cdot \delta_9 = 0$. In the same manner, we can now write such requirements for all the deltas:

$$
\begin{aligned}
\delta_3 \cdot \delta_9 &= 0 \\
\delta_4 \cdot \delta_8 &= 0 \\
\delta_1 \cdot \delta_7 &= 0 \\
\delta_2 \cdot \delta_6 &= 0 \\
\delta_1 \cdot \delta_6 &= 0 \\
\delta_2 \cdot \delta_7 &= 0 \\
\delta_9 \cdot \delta_4 &= 0 \\
\delta_3 \cdot \delta_8 &= 0
\end{aligned}
\tag{72}
$$

The system of equations above has four solutions:

$$[\delta_1, \delta_2, \delta_3, \delta_4, \delta_6, \delta_7, \delta_8, \delta_9] = [\delta_1, \delta_2, \delta_3, \delta_4, 0, 0, 0, 0] \tag{73}$$

$$[\delta_1, \delta_2, \delta_3, \delta_4, \delta_6, \delta_7, \delta_8, \delta_9] = [\delta_1, \delta_2, 0, 0, 0, 0, \delta_8, \delta_9] \tag{74}$$

$$[\delta_1, \delta_2, \delta_3, \delta_4, \delta_6, \delta_7, \delta_8, \delta_9] = [0, 0, \delta_3, \delta_4, \delta_6, \delta_7, 0, 0] \tag{75}$$

$$[\delta_1, \delta_2, \delta_3, \delta_4, \delta_6, \delta_7, \delta_8, \delta_9] = [0, 0, 0, 0, \delta_6, \delta_7, \delta_8, \delta_9] \tag{76}$$

If we construct the matrix Γ from P (79) we can extract the submatrix contain-

ing the PR part with the variables $x1, x3, ...$:

$\Gamma_{PR} =$

	1	A_0^0	A_0^1	A_1^0	A_1^1	B_0^0	B_0^1	B_1^0	B_1^1
1	1	$a+\delta_1$	$a+\delta_2$	$a+\delta_6$	$a+\delta_7$	$a+\delta_3$	$a+\delta_4$	$a+\delta_8$	$a+\delta_9$
A_0^0	$a+\delta_1$	$a+\delta_1$	$x1$	$x3$	$x4$	a	0	a	0
A_0^1	$a+\delta_2$	$x1$	$a+\delta_2$	$x7$	$x8$	0	a	0	a
A_1^0	$a+\delta_6$	$x3$	$x7$	$a+\delta_6$	$x13$	a	0	0	a
A_1^1	$a+\delta_7$	$x4$	$x8$	$x13$	$a+\delta_7$	0	a	a	0
B_0^0	$a+\delta_3$	a	0	a	0	$a+\delta_3$	$x16$	$x18$	$x19$
B_0^1	$a+\delta_4$	0	a	0	a	$x16$	$a+\delta_4$	$x22$	$x23$
B_1^0	$a+\delta_8$	a	0	0	a	$x18$	$x22$	$a+\delta_8$	$x28$
B_1^1	$a+\delta_9$	0	a	a	0	$x19$	$x23$	$x28$	$a+\delta_9$

Again, it is enough to investigate the reduced matrix of Γ_{PR}. If we rename the two remaining variables to u and v we get the following:

$\Gamma_{PR,r} =$

	1	A_0^0	A_0^1	B_0^0	B_0^1
1	1	$a+\delta_1$	$a+\delta_6$	$a+\delta_3$	$a+\delta_8$
A_0^0	$a+\delta_1$	$a+\delta_1$	u	a	a
A_0^1	$a+\delta_6$	u	$a+\delta_6$	a	0
B_0^0	$a+\delta_3$	a	a	$a+\delta_3$	v
B_0^1	$a+\delta_8$	a	0	v	$a+\delta_8$

(77)

If we substitute the solutions from 73 we get

$\Gamma'_{PR,r} =$

	1	A_0^0	A_0^1	B_0^0	B_0^1
1	1	$a+\delta_1$	a	$a+\delta_3$	a
A_0^0	$a+\delta_1$	$a+\delta_1$	u	a	a
A_0^1	a	u	a	a	0
B_0^0	$a+\delta_3$	a	a	$a+\delta_3$	v
B_0^1	a	a	0	v	a

(78)

Here are the minors:

$$\begin{aligned}
\Gamma_{1,2,3,4,5} &= -2u^2a^2v - u^2a^2 - \delta_1\delta_3^2a^2 - 2\delta_3u^2av + u^2\delta_3^2a - 2\delta_1uav^2 + 2\delta_1ua^2v \\
&\quad +2a^2uv\delta_3 - a^2v^2 + u^2v^2 + 2ua^3 + 2a^3v + \delta_1\delta_3a^2 - \delta_1av^2 - u^2\delta_3a \\
&\quad -2ua^2v - a^4 + 3\delta_1a^2v^2 - 2ua^2v^2 + 6ua^3v - \delta_1^2\delta_3a^2 + \delta_1^2av^2 - 2\delta_1a^3v \\
&\quad -2u\delta_3a^3 + 2a^5 + 2a^3v^2 - 4a^4v - 4ua^4 + 2u^2a^3 + 3u^2\delta_3a^2 \\
\Gamma_{2,3,4,5} &= -a^2v^2 + \delta_1\delta_3a^2 - \delta_1av^2 - u^2a^2 - u^2\delta_3a + u^2v^2 + 2ua^3 - 2ua^2v - a^4 + 2a^3v \\
\Gamma_{3,4,5} &= \delta_3a^2 - av^2 \\
\Gamma_{4,5} &= a^2 + \delta_3a - v^2
\end{aligned}$$

Since the following equation system

$$\begin{aligned}
\Gamma_{1,2,3,4,5} &\geq 0 \\
\Gamma_{2,3,4,5} &\geq 0 \\
\Gamma_{3,4,5} &\geq 0 \\
\Gamma_{4,5} &\geq 0
\end{aligned}$$

has no solution we have that $\Gamma'_{PR,r}$ (78) is not positive semidefinite which implies that Γ_{PR} is not, neither. It is easy to show that for all of the four solutions above, $\Gamma_{PR,r}$ is not positive semidefinite, which means that P (79) can not be implemented by the means of quantum mechanics.

Lemma 10.5. *Any P containing a box as in 79 can not be implemented by the means of quantum mechanics.*

Proof: Also here, by the construction of the matrix Γ we can extract the submatrix corresponding to 79 from which we know that it is not positive semidefinite.

□

In the section about binary output we have seen a box P (88) which is also not implementable. Let us have a look at this box, embedded in a box with output dimension three.

$P =$

		0			1		
		0	1	Δ	0	1	Δ
0	0	a	0	δ_1	a	0	δ_1
	1	0	a	δ_2	0	a	δ_2
	Δ	δ_3	δ_4	δ_5	δ_8	δ_9	δ_{10}
1	0	a	0	δ_6	p	ε	δ_6
	1	0	a	δ_7	ε	p	δ_7
	Δ	δ_3	δ_4	δ_{11}	δ_8	δ_9	δ_{12}

(79)

with

$$p = a - \varepsilon \quad (80)$$

$$\varepsilon > 0 \quad (81)$$

Let now $P \in P_{not-disc}$ except for $(x, y) = (1, 1)$. We now want to have a look at the values $p, \varepsilon, \delta_6, \delta_7, \delta_8, \delta_9, \delta_{12}$, given all the other probabilities of P. There are the following possible cases:

Definition 10.6. *The four cases are:*

1. $p \neq 0$
2. $p = 0, Equations(72) \neq 0$
3. $p = 0, Equations(72) = 0, \varepsilon = 0$
4. $p = 0, Equations(72) = 0, \varepsilon \neq 0$

10.4 The Case of Input and Ouput greater than 2

Definition 10.7. *A box P is called 4feasible if and only if all possible subboxes P' of P with $|X| = |Y| = 2$ (called 4-tuple) of input pairs are feasible. The box is called 4infeasible if there exists at least one such 4-tuple which is infeasible.*

Conjecture 10.8. *Assume we are at some point t of the opening process of a box P for which holds that the box is, at the moment of t, 4feasible and that the box enables a local-deterministic strategy not only covering output being discarded. Further assume that opening a next input pair, point t', sets the box in a state where it is still 4feasible. This means that there still exists a local-deterministic strategy for the new box.*

From *Claim 10.8* it would follow that if we are at point t', having a box P preventing a local-deterministic strategy, the box is either $4infeasible$, or, at a point before, t, it already prevented such a strategy.This could be used in order to show that we can not generate a perfectly common secret bit with a single usage of a box: Assume we have a secure box which is $4feasible$. This means that if we remove an input-output pair, the box is still secure. As the box was $4feasible$ in the original state, it stays so, no matter which part of the box we remove. Thus, we have that the box, at another step before, was already secure. If we would continue, we would finally get to a box with input dimension 2 which would be secure and feasible, but we know that this is not possible.

10.4.1 Example

Consider the following box for which there does not exist a box partition attack. All the input pairs belonging to P_{disc} are indicated by the empty boxes. Let us now, for example, start with the three input pairs $(2,3),(3,3)$ and $(3,4)$ with a possible grid indicated by the lightgray shaded boxes.

$P =$

		0			1			2			3			4		
		0	1	δ	0	1	δ	0	1	δ	0	1	δ	0	1	δ
0	0	a	0	0	a	0	0	□	□	□	□	□	□	0	a	0
	1	0	a	δ_2	0	a	δ_2	□	□	□	□	□	□	a	0	δ_2
	δ	0	δ_1	0	0	δ_1	0	□	□	□	□	□	□	0	δ_1	0
1	0	a	0	0	a	0	0	a	0	0	□	□	□	□	□	□
	1	0	a	δ_2	0	a	δ_2	0	a	δ_2	□	□	□	□	□	□
	δ	0	δ_1	0	0	δ_1	0	0	δ_1	0	□	□	□	□	□	□
2	0	□	□	□	a	0	0	a	0	0	a	0	0	□	□	□
	1	□	□	□	0	a	δ_2	0	a	δ_2	0	a	δ_2	□	□	□
	δ	□	□	□	0	δ_1	0	0	δ_1	0	0	δ_1	0	□	□	□
3	0	□	□	□	□	□	□	a	0	0	a	0	0	a	0	0
	1	□	□	□	□	□	□	0	a	δ_2	0	a	δ_2	0	a	δ_2
	δ	□	□	□	□	□	□	0	δ_1	0	0	δ_1	0	0	δ_1	0
4	0	0	a	0	□	□	□	□	□	□	a	0	0	a	0	0
	1	a	0	δ_2	□	□	□	□	□	□	0	a	δ_2	0	a	δ_2
	δ	0	δ_1	0	□	□	□	□	□	□	0	δ_1	0	0	$\delta 4$	0

(82)

Input pair $(2,4)$ might correspond to Case 1 (see *Definition 10.6*):

$P =$

		0			1			2			3			4		
		0	1	δ	0	1	δ	0	1	δ	0	1	δ	0	1	δ
0	0	a	0	0	a	0	0	□	□	□	□	□	□	0	a	0
	1	0	a	δ_2	0	a	δ_2	□	□	□	□	□	□	a	0	δ_2
	δ	0	δ_1	0	0	δ_1	0	□	□	□	□	□	□	0	δ_1	0
1	0	a	0	0	a	0	0	a	0	0	□	□	□	□	□	□
	1	0	a	δ_2	0	a	δ_2	0	a	δ_2	□	□	□	□	□	□
	δ	0	δ_1	0	0	δ_1	0	0	δ_1	0	□	□	□	□	□	□
2	0	□	□	□	a	0	0	a	0	0	a	0	0	a	0	0
	1	□	□	□	0	a	δ_2	0	a	δ_2	0	a	δ_2	0	a	δ_2
	δ	□	□	□	0	δ_1	0	0	δ_1	0	0	δ_1	0	0	δ_1	0
3	0	□	□	□	□	□	□	a	0	0	a	0	0	a	0	0
	1	□	□	□	□	□	□	0	a	δ_2	0	a	δ_2	0	a	δ_2
	δ	□	□	□	□	□	□	0	δ_1	0	0	δ_1	0	0	δ_1	0
4	0	0	a	0	□	□	□	□	□	□	a	0	0	a	0	0
	1	a	0	δ_2	□	□	□	□	□	□	0	a	δ_2	0	a	δ_2
	δ	0	δ_1	0	□	□	□	□	□	□	0	δ_1	0	0	$\delta 4$	0

(83)

As a next step we might add input pairs $(1,2)$ and $(2,2)$. Because of the non-signaling condition, if we land in Case 2 we would automatically also land in Case 4. So we can land either in Case 1 or in Case 3. For Case 3 we would need $P(\delta,0|1,3) = a$ and $P(\delta,1|1,3) = a + \delta_1$ which would make the box signalling, as $\sum_{b=0}^{\delta} P(\delta,b|1,2) = \delta_1 < \sum_{b=0}^{\delta} P(\delta,b|1,3) = 2 \cdot a + \delta_1$. Therefore, the only case left preserving the partition attack is Case 1. From here it is easy to see that if $(1,4)$ is opened in Case 1, we automatically would have a case 4 for $(0,1),(1,1),(0,4)$ and $(1,4)$ which would make the whole box secure but infeasible.

10.4.2 Second Example

Let us consider the following box P, for which there exists a partition attack. All the input pairs belonging to P_{disc} are indicated by the empty boxes. Let us now, for example, start with the three input pairs $(2,3),(3,3)$ and $(3,4)$ with a possible grid indicated by the lightgray shaded boxes.

$$P \;=$$

		0			1			2			3			4		
		0	1	δ	0	1	δ	0	1	δ	0	1	δ	0	1	δ
0	0	a	0	0	a	0	0	□	□	□	□	□	□	0	a	0
	1	0	a	0	0	a	0	□	□	□	□	□	□	a	0	0
	δ	0	δ_1	0	0	δ_1	0	□	□	□	□	□	□	0	δ_1	0
1	0	a	0	0	a	0	0	a	0	0	□	□	□	□	□	□
	1	0	a	0	0	a	0	0	a	0	□	□	□	□	□	□
	δ	0	δ_1	0	0	δ_1	0	δ_2	δ_3	δ_4	□	□	□	□	□	□
2	0	□	□	□	a	0	0	a	0	0	a	0	0	□	□	□
	1	□	□	□	0	a	0	0	a	0	0	a	0	□	□	□
	δ	□	□	□	0	δ_1	0	δ_2	δ_3	δ_4	δ_2	δ_3	δ_4	□	□	□
3	0	□	□	□	□	□	□	a	0	0	a	0	0	a	0	0
	1	□	□	□	□	□	□	0	a	0	0	a	0	0	a	0
	δ	□	□	□	□	□	□	δ_2	δ_3	δ_4	δ_2	δ_3	δ_4	0	δ_1	0
4	0	0	a	0	□	□	□	□	□	□	a	0	0	a	0	0
	1	a	0	0	□	□	□	□	□	□	0	a	0	0	a	0
	δ	0	δ_1	0	□	□	□	□	□	□	δ_2	δ_3	δ_4	0	δ_1	0

(84)

Input pair $(2, 4)$ might correspond to Case 1:

$$P \;=$$

		0			1			2			3			4		
		0	1	δ	0	1	δ	0	1	δ	0	1	δ	0	1	δ
0	0	a	0	0	a	0	0	□	□	□	□	□	□	0	a	0
	1	0	a	0	0	a	0	□	□	□	□	□	□	a	0	0
	δ	0	δ_1	0	0	δ_1	0	□	□	□	□	□	□	0	δ_1	0
1	0	a	0	0	a	0	0	a	0	0	□	□	□	□	□	□
	1	0	a	0	0	a	0	0	a	0	□	□	□	□	□	□
	δ	0	δ_1	0	0	δ_1	0	δ_2	δ_3	δ_4	□	□	□	□	□	□
2	0	□	□	□	a	0	0	a	0	0	a	0	0	a	0	0
	1	□	□	□	0	a	0	0	a	0	0	a	0	0	a	0
	δ	□	□	□	0	δ_1	0	δ_2	δ_3	δ_4	δ_2	δ_3	δ_4	0	δ_1	0
3	0	□	□	□	□	□	□	a	0	0	a	0	0	a	0	0
	1	□	□	□	□	□	□	0	a	0	0	a	0	0	a	0
	δ	□	□	□	□	□	□	δ_2	δ_3	δ_4	δ_2	δ_3	δ_4	0	δ_1	0
4	0	0	a	0	□	□	□	□	□	□	a	0	0	a	0	0
	1	a	0	0	□	□	□	□	□	□	0	a	0	0	a	0
	δ	0	δ_1	0	□	□	□	□	□	□	δ_2	δ_3	δ_4	0	δ_1	0

(85)

As a next step we might add input pairs $(1,2)$ and $(2,2)$ in order to land, for example, in Case 2:

$P =$

		0			1			2			3			4		
		0	1	δ	0	1	δ	0	1	δ	0	1	δ	0	1	δ
0	0	a	0	0	a	0	0	□	□	□	□	□	□	0	a	0
	1	0	a	0	0	a	0	□	□	□	□	□	□	a	0	0
	δ	0	δ_1	0	0	δ_1	0	□	□	□	□	□	□	0	δ_1	0
1	0	a	0	0	a	0	0	a	0	0	0	a	0	□	□	□
	1	0	a	0	0	a	0	0	a	0	a	0	0	□	□	□
	δ	0	δ_1	0	0	δ_1	0	δ_2	δ_3	δ_4	δ_2	δ_3	δ_4	□	□	□
2	0	□	□	□	a	0	0	a	0	0	a	0	0	a	0	0
	1	□	□	□	0	a	0	0	a	0	0	a	0	0	a	0
	δ	□	□	□	0	δ_1	0	δ_2	δ_3	δ_4	δ_2	δ_3	δ_4	0	δ_1	0
3	0	□	□	□	□	□	□	a	0	0	a	0	0	a	0	0
	1	□	□	□	□	□	□	0	a	0	0	a	0	0	a	0
	δ	□	□	□	□	□	□	δ_2	δ_3	δ_4	δ_2	δ_3	δ_4	0	δ_1	0
4	0	0	a	0	□	□	□	□	□	□	a	0	0	a	0	0
	1	a	0	0	□	□	□	□	□	□	0	a	0	0	a	0
	δ	0	δ_1	0	□	□	□	□	□	□	δ_2	δ_3	δ_4	0	δ_1	0

(86)

In this example, Case 2 does not make the whole box infeasible, but, on the other hand, it destroys our partition attack. Never the less, we can change the whole grid:

$P =$

		0			1			2			3			4		
		0	1	δ	0	1	δ	0	1	δ	0	1	δ	0	1	δ
0	0	a	0	0	a	0	0	□	□	□	□	□	□	0	a	0
	1	0	a	0	0	a	0	□	□	□	□	□	□	a	0	0
	δ	0	δ_1	0	0	δ_1	0	□	□	□	□	□	□	0	δ_1	0
1	0	a	0	0	a	0	0	a	0	0	0	a	0	□	□	□
	1	0	a	0	0	a	0	0	a	0	a	0	0	□	□	□
	δ	0	δ_1	0	0	δ_1	0	δ_2	δ_3	δ_4	δ_2	δ_3	δ_4	□	□	□
2	0	□	□	□	a	0	0	a	0	0	a	0	0	a	0	0
	1	□	□	□	0	a	0	0	a	0	0	a	0	0	a	0
	δ	□	□	□	0	δ_1	0	δ_2	δ_3	δ_4	δ_2	δ_3	δ_4	0	δ_1	0
3	0	□	□	□	□	□	□	a	0	0	a	0	0	a	0	0
	1	□	□	□	□	□	□	0	a	0	0	a	0	0	a	0
	δ	□	□	□	□	□	□	δ_2	δ_3	δ_4	δ_2	δ_3	δ_4	0	δ_1	0
4	0	0	a	0	□	□	□	□	□	□	a	0	0	a	0	0
	1	a	0	0	□	□	□	□	□	□	0	a	0	0	a	0
	δ	0	δ_1	0	□	□	□	□	□	□	δ_2	δ_3	δ_4	0	δ_1	0

(87)

In the same manner we can continue and we would see that we never land in Case 4.

11 Epsilon Security

In cryptography, we often do not require perfect secrecy, which suggests the investigation of boxes where the part not getting discarded does not contain perfect correlation or anti-correlation but values comprising a small error. In the case of binary input and output, a PR box with errors would look like this:

$$P = \begin{array}{cc|cc|cc|cc} & & \multicolumn{2}{c|}{0} & \multicolumn{2}{c}{1} \\ & & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & \frac{1}{2}-\mu_1 & \mu_1 & \frac{1}{2}-\mu_2 & \mu_2 \\ & 1 & \mu_1 & \frac{1}{2}-\mu_1 & \mu_2 & \frac{1}{2}-\mu_2 \\ \hline 1 & 0 & \frac{1}{2}-\mu_3 & \mu_3 & \mu_4 & \frac{1}{2}-\mu_4 \\ & 1 & \mu_3 & \frac{1}{2}-\mu_3 & \frac{1}{2}-\mu_4 & \mu_4 \end{array} \tag{88}$$

Let us assume that the only output used for bit agreement is for input $x = y = 0$. It seems to be an interesting question to see how small we can make μ_1 for correctness, still preventing a box-partition attack as well as possible, for secrecy. The local-part of a box can be quantified as follows:

$$Locality(P) = 2 \cdot \sum_{i=1}^{4} \mu_i \tag{89}$$

Obvioulsy, we want to keep locality as small as possible as the more local the box is, the more a partition attack gets enabled, resulting in a more insecure box. This leads us to the following problem of semidefinite programming, where for a given μ_1 we try to minimize the locality under the constraint that the Γ matrix is positive semidefinite:

For a given μ_1 :

$$\begin{array}{l} \min(\sum_{i=2}^{4} \mu_i) \\ \text{subject to} \\ \Gamma_P \succeq 0 \end{array}$$

In order to solve this problem, we made use of a free toolbox for MATLAB called YALMIP [5], a modelling language for defining and solving optimization problems. The results are listed in the table below:

μ_1	Locality
0.1	0.5904
0.01	0.6507
0.001	0.7136
0.0001	0.7380
0.00001	0.7462
0.000001	0.7488

(90)

As we can see in the table above, there seems to be a tradeoff between secrecy and correctness, namely the better the correlation we have, the worse secrecy gets.

12 Conclusion and Further Work

Even though, at a first glance, the concept of quantum pseudo telepathy seemed to be a promising way, we have seen that, even in addition to discard of input, it does not help on establishing perfect secrecy by the means of quantum mechanics. We have learned that, in the case of binary output, in order to get perfectly correlated and perfectly secret bits, we would need maximal non-locality which prohibits any quantum simulation.
It would be interesting to see wheather we would be able to gain more secrecy in the case of input and output dimensions being both greater than two. Additionally, as we often do not require perfect secrecy in cryptography, it would be newsworthy to investigate systems not containing perfect correlation or anti-correlation, but comprising small errors.

References

[1] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signalling and quantum key distribution. *Physical Review Letters*, 95:010503, 2005.

[2] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *FOUNDATIONS OF PHYSICS*, 11:1877, 2004.

[3] Roger Colbeck and Renato Renner. Hidden variable models for quantum theory cannot have any local part. *Physical Review Letters*, 101(5), 2008.

[4] Esther Hänggi, Renato Renner, and Stefan Wolf. The impossibility of non-signaling privacy amplification. 2007.

[5] J. Löfberg. Yalmip : A toolbox for modeling and optimization in MATLAB. In *Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004.

[6] Miguel Navascues, Stefano Pironio, and Antonio Acin. Bounding the set of quantum correlations. *Physical Review Letters*, 98:010401, 2007.

[7] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, October 2000.